COMP6300

Applied Cryptography

Session 2, Special circumstance 2020

Department of Computing

Contents

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and ot her small group learning activities on campus for the second half-year, while keeping an online ver sion available for those students unable to return or those who choose to continue their studies onli ne.

To check the availability of face-to-face and onlin e activities for your unit, please go to timetable vi ewer. To check detailed information on unit asses sments visit your unit's iLearn space or consult yo ur unit convenor.

General Information

Unit convenor and teaching staff
Convenor and Lecturer
Les Bell
les.bell@mq.edu.au
TBA - email to make appointment.

Tutor
Mohamadali Mehrabi
mohamadali.mehrabi@mq.edu.au
TBA

Tutor
Salma Hamad
salma.hamad@mq.edu.au
TBA

Credit points
10

Prerequisites

Corequisites

Co-badged status
COMP2300

Unit description
This unit provides an introduction to modern applied cryptography. It deals with the concepts and techniques behind cryptographic primitives, such as hash functions, symmetric-key ciphers, public-key cryptography and digital signatures. It then explains the concept of cryptanalysis before addressing important cryptographic protocols. The unit concludes with a review of existing applications including blockchain and cryptocurrencies, electronic voting schemes, executable code signing, full disk encryption, etc.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

On successful completion of this unit, you will be able to:

ULO1: Explain the concepts and principles on which modern cryptography relies upon.

ULO2: Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign messages.

ULO3: Decipher simple encrypted messages using a range of cryptanalysis methods.

ULO4: Apply cryptographic technologies and protocols to increase data security and protect privacy.

General Assessment Information

Late Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total.

Under no circumstances will submissions will be accepted after solutions have been posted.

Module Examinations

Module Examinations will be scheduled during lecture timeslots in weeks 5, 9 and 13. Your attention is drawn to the university's 'Fit to Sit' policy, which states that by commencing an examination you are certifying yourself as fit to sit that examination. In particular, if you commence a Module Examination late, with insufficient time to finish it, you will *not* be offered a Supplementary Examination.

Supplementary Examinations

Applications for Supplementary Examinations under the Disruption to Studies Policy must be made via AskMQ. If this is approved, the Unit Convenor will *attempt* to schedule an examination at a time convenient to the student and will notify the student of the date and time of the examination in a timely fashion.

Assessment Tasks

Name	Weighting	Hurdle	Due
Tutorial Tasks	10%	Yes	Weekly
Module Examination 1	20%	No	Week 5
Module Examination 2	20%	No	Week 9
Module Examination 3	20%	No	Week 13
Assignment 1	15%	No	Week 7

Name	Weighting	Hurdle	Due
Assignment 2	15%	No	Week 12

Tutorial Tasks

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 6 hours
Due: **Weekly**
Weighting: **10%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

Each week, a set of exercises will be available online. Some require written submissions, while some are multiple choice. Your solutions should be submitted electronically via iLearn before the deadline specified in the text.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign messages.
- Decipher simple encrypted messages using a range of cryptanalysis methods.
- Apply cryptographic technologies and protocols to increase data security and protect privacy.

Module Examination 1

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 5**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 5 during practical class. This will test your understanding of material covered in weeks 1 to 4.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign

messages.

- Decipher simple encrypted messages using a range of cryptanalysis methods.

Module Examination 2

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 9**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 9 during practical class. This will test your understanding of material covered in weeks 5 to 8.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Apply cryptographic technologies and protocols to increase data security and protect privacy.

Module Examination 3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Week 13**
Weighting: **20%**

A 50 minutes long written examination worth 20% that will be held in week 13 during practical class. This will test your understanding of material covered in weeks 9 to 12.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Apply cryptographic technologies and protocols to increase data security and protect privacy.

Assignment 1

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 7**
Weighting: **15%**

This assignment deals with symmetric-key cryptography and is due on week 7. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Explain the concepts and principles on which modern cryptography relies upon.
- Employ adapted cryptographic tools and techniques to encrypt, decrypt and sign messages.
- Decipher simple encrypted messages using a range of cryptanalysis methods.

Assignment 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 12**
Weighting: **15%**

This assignment deals with public-key cryptography and is due on week 12. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Apply cryptographic technologies and protocols to increase data security and protect privacy.

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Delivery and Resources

Computing Facilities

Important! Please note that this is a BYOD (Bring Your Own Device) unit. You are expected to use your own computer (Windows, Mac or Linux) to complete the workshops, install and

configure the required software, and incorporate secure practices into your daily work (and play!) routines.

Classes

Each week you should complete any assigned readings before viewing the lecture material. The lectures will be delivered as pre-recorded videos - the lengths will vary but there will be approximately three hours of lecture content each week

There will also be a one-hour workshop every week, which will be offered both in on-campus and online (Zoom meeting) formats. The workshops use hands-on exercises to reinforce concepts introduced during the lectures. You will find it helpful to read the workshop instructions before starting- that way, you can get to work quickly!

Note that workshops commence in week 1.

Please also note that you will be required to submit work each week. Failure to do so may result in your failing the unit or being excluded from examinations.

Discussion Boards

This unit makes use of discussion boards hosted within iLearn. Please post questions there; they are monitored by the staff on the unit. Asking - and answering - questions is one of the most effective ways of learning.

Required and Recommended Texts and/or Materials

Required Textbook

- Easttom, Chuck. Modern Cryptography: Applied Mathematics for Encryption and Information Security. 1 edition. New York: McGraw-Hill Education, 2015. The book is available in online format through the Library; there will be allocated readings each week.

Recommended Supplementary Texts

- Anderson, Ross J. Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed. Wiley, 2010.
- Menezes, A.J., P. C. van Oorrschot and S. A. Vanstone, Handbook of applied cryptography (HAC), CRC Press, Boca Raton, FL, 1996. All required chapters are available online at http://cacr.uwaterloo.ca/hac/
- Smart, N., Cryptography Made Simple, Springer Verlag,
- NIST SP 800 documents available from http://csrc.nist.gov/publications/PubsSPs.html
- IETF RFC's available from http://www.rfc-editor.org
- Bauer, Craig P., Secret History: The Story of Cryptology, CRC Press (2013)
- Ferguson, Neils, Tadayoshi Kohno and Bruce Schneier, Cryptography Engineering: Design Principles and Practical Applications, 1st ed., Wiley

There will be other readings, but links or references will be posted on iLearn

Technology Used and Required

iLearn

iLearn is a Learning Management System that gives you access to lecture slides, lecture recordings, forums, assessment tasks, instructions for practicals, discussion forums and other resources.

Crypto Technology and Tools

Java, Python or C++ programming language and GP/PARI, VeraCrypt, Thunderbird, Gnu Privacy Guard, Enigmail, OpenSSH, PuTTY, Ophcrack.

Unit Schedule

Week	Lecture Content
1	Introduction; Classical Crypto; Information Theory, Number Theory
2	Symmetric block ciphers & Intro to Assignment 1
3	Keystreams and stream ciphers
4	Hashes and Digests
5	Number Theory, PKC (RSA, D-H, El Gamal and DSA)
6	Elliptic Curve Cryptography
7	Digital Signatures
8	Hybrid Cryptosystems and Network Security
9	Protocols; Cryptanalysis of Symmetric Cryptosystems
10	Cryptanalysis of Public Key Cryptosystems
11	Attacking protocols; Quantum Crypto and Post-Quantum Crypto
12	Zero Knowledge Proofs, Electronic Voting and Cryptocurrencies
13	Revision

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy

- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Students seeking more policy resources can visit the Student Policy Gateway (https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/study/getting-started/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides

- Ask a Librarian

Student Services and Support

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Changes from Previous Offering

The required textbook has been changed, and workshops re-aligned to allow both on-campus and online participation.